International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 153-164

SECURE AND FAST DATA TRANSFER: WITH NETWORK CODING

ASHVINI JADHAV[1] & SHRINIWAS GADAGE[2]

[1]ME(Computer Network), Pune University, Maharashtra, India

[2]GH Raisoni College of Engineering and Management, University of Pune, Maharashtra, India

ABSTRACT

The theory of network coding promises significant benefits in network performance, especially in lossy networks and in multicast and multipath scenarios. To realize these benefits in practice, we need to understand how coding across packets interacts with the acknowledgment (ACK)-based flow control mechanism that forms a central part of today's Internet protocols such as transmission control protocol (TCP). The mechanism for TCP/NC that incorporates network coding into TCP with only minor changes to the protocol stack, thereby allowing incremental deployment. how the source transmits linear combinations of packets currently in the congestion window. And new interpretation of ACKs the sink acknowledges every degree of freedom even if it does not reveal an original packet immediately. Thus, new TCP ACK rule takes into account the network coding operations in the lower layer and enables a TCP-compatible sliding-window approach to network coding. Coding essentially masks losses from the congestion control algorithm and allows TCP/NC to react smoothly to losses, resulting in a novel and effective approach for congestion control over lossy networks such as wireless networks

KEYWORDS: AES, ACO, Butterfly Network, TCP/NC

INTRODUCTION

Wireless networks and communications have emerged as a dominant mode of communications, technical advances in wireless communications has brought faster and more affordable network access. However, the technological advances are often matched, if not outmatched, by users appetite for even faster, cheaper, and more robust wireless networks. For instance, with the rise of new forms of data, in particular high quality multimedia, we are faced with a challenge of transforming our communication networks to handle unparalleled growth in traffic and strict delay constraints. In order to meet the future demands, we need to manage the existing wireless networks more efficiently in terms of, but not exclusively, energy, latency, and bandwidth; and to build new infrastructure and design novel protocols that take into account the high-bandwidth, dynamic, and di- verse traffic that needs to be served across wired and wireless medium. There are several sources of challenges in designing a robust wireless networks, which are not as prominent in wired networks.

- Wireless is a shared medium They ultimately have to share either in time, frequency, or space. When senders and receivers fail to share the wireless medium appropriately, we observe a collision or an interference, which hinders efficient communication.
- Wireless is stochastic in nature The time varying nature of wireless results in not only ever-changing capacity and delay but also errors and erasures.
- Wireless is a broadcast medium Wireless networks are often insecure, prone to adversarial eavesdropping and contamination attacks.

These properties of wireless make designing and operating wireless networks vastly different from those of wired networks. However, our currently deployed wireless networks not adequately address these problems. Often measures to address the problems of wireless networks are appended to the existing architecture. For instance, the current design to combat erasures and errors is retransmission

Motivation

Motivated by these observations, propose system build more efficient, high performance wireless networks. In this dissertation, Present algorithms that can better manage interference, overcome losses, and provide secure communications by recognizing and harnessing the characteristics of wireless.

Key Idea

The key idea behind this dissertation is in understanding that wireless networks are fundamentally different from wired networks, and recognizing that directly applying techniques from wired networks to wireless networks limits throughput and performance. Network coding promises a fundamentally new way to operate networks. At present, the intermediate nodes can only store, forward, or replicate the information they receive. This store-and-forward approach is closely related to the multi-commodity flow problem, and has been studied extensively owing to its wide applications to communication networks. network coding questions the fundamental assumption in our store and forward network designs. The theory of network coding, first introduced in their seminal paper by Ahlswede et al. [1], breaks the convention of router net- works. Intermediate nodes,

Objective

The objective of the Network Coding can benefit Internet communication. One goal of that improves Internet communication. Another goal is to gather information on the existing practical implementations of NC, common functionalities and propose a path to standardization of communication. To provide fast, secure, reliable and cost effective communicate ion medium between multiple clients and server. To present a simplified server-multiple client architecture which enables multi cast messages with in a public/private channel.

Goal of Paper

The goal of this task is to identify appropriate architectural considerations in applying networking coding techniques in different parts of the operation butterfly network. Modularity of design remains a key element of achieving successful deployment, operation, and maintenance of such systems. This dissertation shows that network coding is a powerful tool that can efficiently and effectively overcome interference, erasures. Network coding can deliver on the promise of a more efficient wireless network with higher throughput and reliability.

OVERVIEW OF NETWORK CODING

Network Coding is a technique that can be used to improve a network throughput, efficiency and scalability, as well as resilience to attacks and eavesdropping, as compared to traditional methods. In Network Coding, data is manipulated inside the network or at the network edges to achieve the maximum possible information flow in a network, based on principles of Shannon Information Theory.

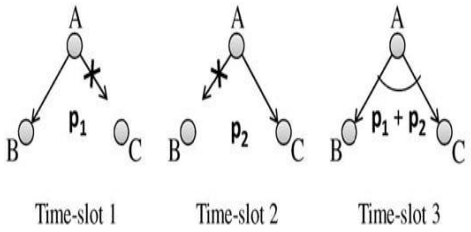

Figure 1: Coding Over a Broadcast[19]

Network Coding Background

Network coding has evolved significantly from its inception. Initially, network coding was proposed for wired multicast networks, in which one or more sources may wish to deliver information to many receivers. References [1] showed that, if additional computing tasks are performed at the intermediate nodes, the multicast capacity can be achieved.

In case of lost the packet, then a simple retransmission strategy may not be the best option, since the retransmission is useless from the viewpoint of the other receivers that have already received the packet. figure1 node A broadcasts 2 packets to nodes B and C. In the first time-slot, only node B receives packet p1 and in the second slot, only node C receives packet p2. At this point, if instead of retransmitting p1 or p2, node A is allowed to mix the information and send a single packet containing the bitwise xor of p1 and p2, then both B and C receive their missing packet in just one additional time slot. This example shows that if allow coding across packets, it is possible to convey new information simultaneously to all connected receivers. as per this example if possible I can send multiple packet in one time slot just like parallel sending broadcasting format

The now standard example is the butterfly network from [1] as per, which is shown in Figure.2. Here, node A wants to multicast a stream of packets to nodes F and G. Assume the links are error free with a capacity of one packet per slot. If all nodes are only allowed to forward packets, then node D can forward either the packet from B p1 xor the one from C p2. It can be seen that alternating between these options gives a multicast throughput of 1.5 packets per slot.

However, if node D sends a bitwise xor of p1 and p2 as shown in the figure, then it is possible to satisfy both receivers simultaneously, resulting in a multicast throughput of two packets per time slot. This is the highest possible, since it meets the min-cut bound for each receiver.

- Through the butterfly network example, Ahlswede et al. [1] introduced the field of network coding. With network coding, a node inside the network, instead of simply forwarding the incoming packets onto outgoing links, is now allowed to send a coded version of the incoming packets.
- Although both the examples above use a bitwise xor code, the coding operation could be much more general
    - The groups of bits as elements of a finite field, and a packet as a vector over this field.
    - Coding could then correspond to performing linear combinations of these vectors, with coefficients chosen from the field of operation.

In order to decode, the receiver will have to collect as many linear combinations as the number of packets that were mixed in, and then solve the resulting system of linear equations by Gauss Jordan elimination. If ACK of packet receive as early as possible it avoid retransmission and it reduce traffic achieving successful deployment, operation, and maintenance of such systems. Thus, it may be useful

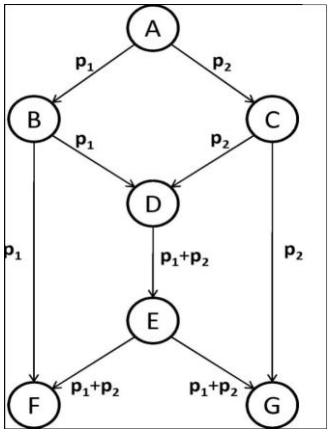

Figure 2: Butterfly Network[19]

Related Activity

In packet-based FEC content to support high assurance delivery of files or other data over unidirectional network path and support of multicast Negative-ACKnowledgement (NACK) based Automatic Repeat-reQuest (ARQ) protocols using packet erasure coding repair strategies. Both of these specifications support the use of different FEC encoding techniques

The following are topics of interest Research:

- Performance bounds of NC and gains over non-NC communication
- Encoding Decoding Reendowing techniques and their performance implications
- Multicasting Problem
- Open Problems in NC research
- Security
- Load balancing
- Reduce packet loss
- Band width utilization
- Congestion Control

Practical implementations, analyze their architecture and identify best/common approaches for the promising NC methods

The following are topics of interest in NC Implementation:

Architectural considerations

The goal of this task is to identify appropriate architectural considerations in applying networking coding techniques in different parts of the operation butterfly network. Modularity of design remains a key element of achieving successful deployment, operation, and maintenance of such systems. Thus, it may be useful to determine some appropriate mapping of different uses of network coding to different system functions. This includes the relationships between data transport, control plane, forwarding plane, and even layer IP and TCP layer components. With emerging Software-Defined Networking (SDN) architecture being proposed and pursued, one topic of interest will be practical ways in which network coding might be

accommodated in such systems. Additionally, SDN systems may actually offer opportunities for practical implementation of network coding concepts.

End-to-End v.s Hop-by-Hop NC

Related to topic 1 (architectural considerations), there are specific considerations for the application of Network Coding for end-to-end versus hop-by-hop (or local scope) encoding and data delivery. For example, employment of Network Coding techniques by intermediate systems implies more sophisticated (stateful and/or complex) operation than typical existing packet forwarding operations. Additionally, the interrelationship between end-to-end delivery and hop-by-hop operations may require a richer interface than the present distinct protocol layers.

Application-Layer NC

In addition to potential refactoring of network layer functionality to include Network Coding, there exists the potential to apply Network Coding as an application-layer technique for distributed data dissemination. Additionally, application-layer coding may be used in tandem with network-layer coding techniques also. There is recent interest in "Content-based" or Information Centric Networking (ICN) and network coding can be a very compatible, supporting mechanism for this alternative form of networking. Additionally, in some cases it is possible for application-layer information encoding (e.g. data compression) and channel coding (i.e., network coding in this case) to be performed jointly for improved performance or utility.

Security

The most non impact to security is for the case when intermediate systems perform network coding operations and may wish to re-encode content for forwarding or delivery. There are cryptographic techniques that can be applied to enable this to be performed in a secure fashion, i.e., without violating end-to-end confidentiality. Such techniques are also being examined in the context of content-based or information-centric networking. There may be other security implications for network coding systems in the area of control plane functions and data integrity that should be examined.

\subsection {Common Encoding Algorithms, Service Descriptions, and Packet Formats}

When Network Coding is applied to Internet systems and possibly applied in different aspects of network operation, there may be utility in common encoding (and decoding) algorithms, service descriptions, and even packet (or other data unit) formats.

Throughput

The throughput of todays wireless net- works is far form optimal. NC increases wireless throughput because 1) It use as broadcast nature coding allows the coders to compress the transmitted packets based on information that are known at various nodes. By matching what each neighbor has with what another neighbor wants, a coder can deliver multiple packets to different sources in a single transmission. This type of transformation is named inter-flow network coding because the coding is done over packets that differ in their next hop, and thus from different flows.

Example: Todays people often listen to music in public places. I can imagine situation in which many people wants to listen to their favorite music using common hot-spots. Efficient bandwidth usage is crucial in this type of scenarios. Let’s consider situation in which two clients are users of this service. Each of them has some songs on their devices and want to listen to a song it does not have. In order to get the song a customer wants it also must present which

songs it already has. So A,B are customers of the service, SA and SB songs which users A and B have on their devices. Now imagine that the user A wants to listen the song SB, and the user B wants to listen the song SA. Instead of sending the separate data streams to both of the users, the service point can broadcast XOR version of the stream. As the result both of the users can easily decode their songs as well as the access point can send half of the data required in the scenario. In this example network coding doubles the throughput.

Reliability

In today's network by reliability we usually mean the retransmission of the packets in case of packet loss. This works quite well in wired networks, but seems to be inefficient in wireless ones. Network coding gives new approach to reliability. As the result of mixing information, there are no special packets. To illustrate it, let's consider example from a traditional approach. Without coding a source needs to know which packets the destination missed in order to retransmit them. In an unreliable environment it may consume some extra bandwidth. If we want to use network coding, we usually do not care about individual packets. A source needs to inform us only if it receives enough packets to encode the transmitted file. There is also one additional benefit, because of improved reliability it also improve throughput of the network (less data needs to be retransmitted).

Monitoring

Network coding can be exploited to better monitor the link loss rate in wire- less networks . Let's consider example shown in 2. In the example nodes A, B, C, D,E,F are sensors while nodes G and F are sinks connected through a high-bandwidth link. When we use net- work coding nodes G and F may receive P1,P2,P1+P2 or nothing depending on the transmission on each link. By sending several rounds of probes from C and B. It observe link loss on all five links simultaneously. which leads to bandwidth and energy savings.

Common Encoding Algorithms, Service Descriptions, and Packet Formats

When Network Coding is applied to Internet systems and possibly applied in different aspects of network operation, there may be utility in common encoding (and decoding) algorithms, service descriptions, and even packet (or other data unit) formats.

Proposed System In this section we introduce our protocol and elaborate on its main functional blocks

- In current system coding decoding delay I try to reduce that delay of decoding packet a) Block level coding decoding,
- Intermediate node is work for reencoding so I will provide security for that
- When multiple paths are used in parallel, one important decision is how much of the traffic needs to be sent through each path. Multiple path Optimization with Fuzzy Logic

Coding Decoding Module

Modification for systems using network coding. 1) The key difference to be dealt with is that under network coding the receiver does not obtain T(s,t) be the maximum possible through- put from node S to node t . By the max-flow mincut theorem(s,t) is upper bounded by the minimum capacity of all cuts, which is the sum of the capacities of the edges on a cut, between these two nodes.

Karl Menger proved that there is always a set of edge-disjoint paths achieving the upper edges) C gives the capacity of each link of E . Let bound in a unidqcast scenario, known as the max- flow min-cut theorem.

Logical Description

In my project proposal is that coding operations occur not only at the end hosts but at intermediate node with 1)encoding decoding 2)Load balancing 3)Security ACK and RTT measurement control using packet loss as a congestion indicator is not well suited to this Situation. However, it is useful to note that the congestion related losses are also made to appear as a longer RTT. Therefore, Need an approach that infers congestion from an increase in RTT. The natural choice is TCP- Suit. TCP- Suit uses a proactive approach to congestion control by inferring the size of the network buffers even before they start dropping packets. The crux of the algorithm is to estimate the round-trip time (RTT) and use this information to find the discrepancy between the expected and actual transmission rate. As congestion arises, buffers start to fill up and the RTT starts to rise, and this is used as the congestion signal. This signal is used to adjust the congestion window and hence the rate. In order to use TCP- Suit correctly in this setting, Need to feed it the fictitiously longer RTT of a degree of freedom that includes the fictitious queuing delay. It introduces a novel RTT estimation algorithm to do this. The sender can note down the transmission time of every linear combination. When an ACK arrives, to which transmission it should be matched in order to compute the RTT match it to the transmission that occurred after the one that triggered the previous ACK. Consider the example shown in The congestion, window is assumed to be 4 packets long. All 4 transmissions are linear combinations of the 4 packets in the window. In this example, the 1st packet is seen because of the 1st transmission. The 2nd and 3rd transmissions are lost, and the 4th transmission causes the 2nd packet to be seen (the discrepancy is because of losses). As far as the RTT estimation is concerned, transmissions 2, 3 and 4 are treated as attempts to convey the 2nd degree of freedom. The RTT for the 2nd packet is therefore computed based on the oldest such attempt, namely the 2nd transmission. In other words, the RTT is the difference between the time of reception of ACK=3 (in Figure 4), and the time of the transmission of (p1 + 2p2 + 2p3+ p4).

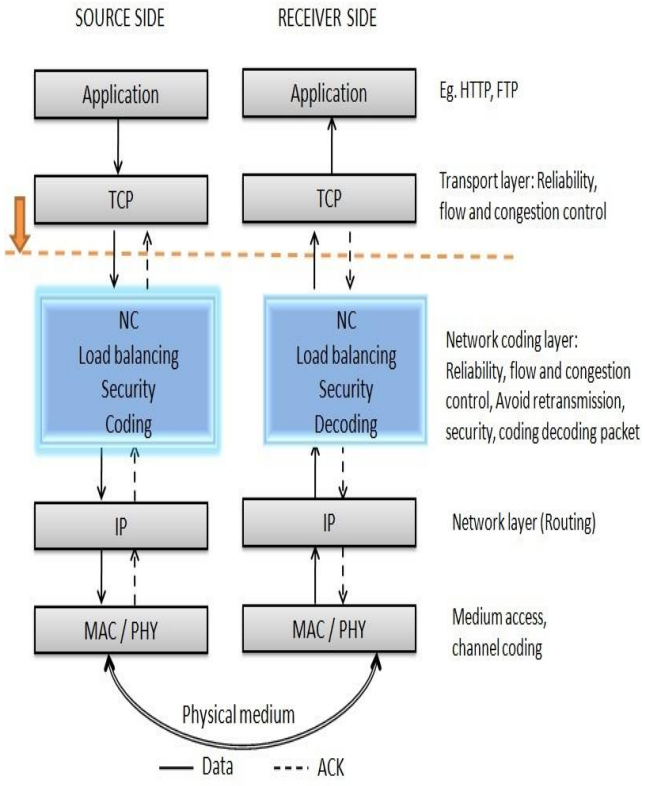

Figure 3: New Protocol Stack

SIMULATION ENVIRONMENT

We have simulated TCPNC by JAVA and compared with TCPNC,TCP-ACO,TCP protocol .

Number of nodes Peer client: 8

Server: 1

Topology node 10 : Butterfly Network

Packet size : 512

The following is the parameters used in the simulations. The network Butterfly network

- Packet loss
- Transmission speed
- Duration simulation
- Sender: IP Address of Sender
- Receiver: Multiple IP Address Receivers

SIMULATION RESULTS

The following graphs shows the simulation results for TCP-ACO, TCPNC,TCP protocol. The Results are compared with TCP-ACO, TCPNC, TCP protocol. Blue line in graph shows results for TCP-ACO protocol Red line in graph shows results for TCPNC protocol and Green line shows results for TCP protocol. From the graphs we come to know that results for TCPNC-ACO algorithm are better than TCP AND TCPNC in each aspect.

CHALLANGES OF SYSTEM

Extensions to Multipath and Multicast: Fur- ther work is needed to ensure that the different characteristics of the paths to the receiver (in case of multipath) or to multiple receivers (in case of multicast) are taken into account correctly by the congestion control algorithm.

Re-Encoding Packets at Intermediate Nodes: The case where intermediate nodes perform network coding. Theory suggests that a lot can be gained by allow-ing intermediate nodes to code as well. Our scheme naturally generalizes to such situations. The ability to code character- istics of the underlying link. Ideally, the choice inside the network is important for multicast connections. of these parameters should be au- tomated. For instance, the Even for a point-to- point connection, the ability to re-correct values could be learned dynamically based on encode at an intermediate node offers the flexibility of measurement of the link characteristics such as the link adding redundancy where it is needed, i.e., just before the loss rate, bandwidth, and de- lay. In addition, the parameters lossy link. The practical aspects of implementing re-have to be extended to cover the case of multipath transport and encoding need to be studied further. Multicast scenarios as well

Automatic Tuning of TCP/NC Parameters: More work is needed in the future for fully understanding the role played by the various parameters of the new protocol, Redundancy factor R and the coding window size W. several useful discussions.

Figure 4

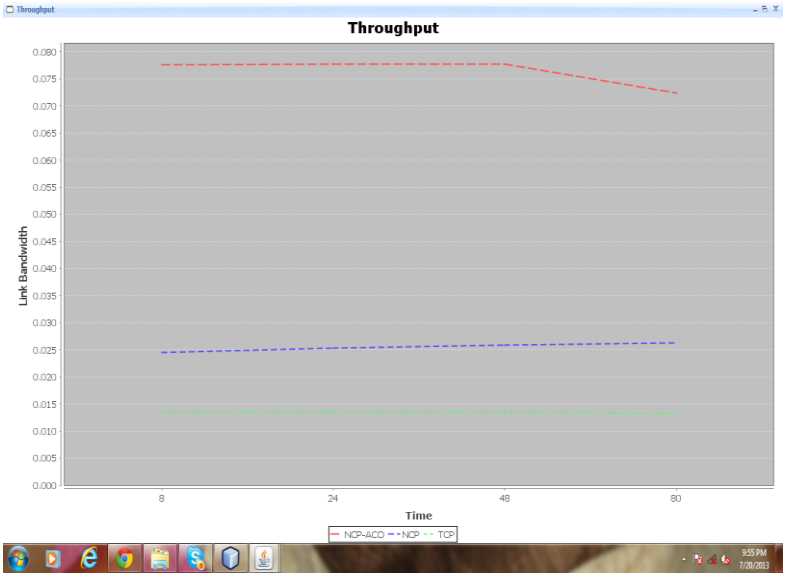

Figure 5: Throughput Wired and wireless Network

CONCLUSIONS

Network coding key role in incorporating coding into the control algorithm. From an implementation perspective, introduce a new net- work coding layer between the network layers on both the source and receiver sides. Thus, changes can be easily deployed in an existing system. A salient feature of proposal is that coding operations occur only at the end hosts, thereby preserving the end-to- end philosophy of TCP. The overhead associated with the coding operations in a practical setting. Throughput gains are seen even though the intermediate nodes do not perform any coding. Theory suggests that a lot can be gained by allowing intermediate nodes to code as well.

Quantifying the impact of such coding is of interest in the future. It presents a new framework for combining coding with feedback based rate-control mechanisms in a practical way. It is of interest to extend this approach to more general settings such as net- work coding based multicast over a general network 1) A feature of previous proposal is that coding operations occur only at the end hosts 2) In my project proposal is that coding operations occur not only at the end hosts but at intermediate node with 1) encoding decoding 2) Load balancing 3)Security

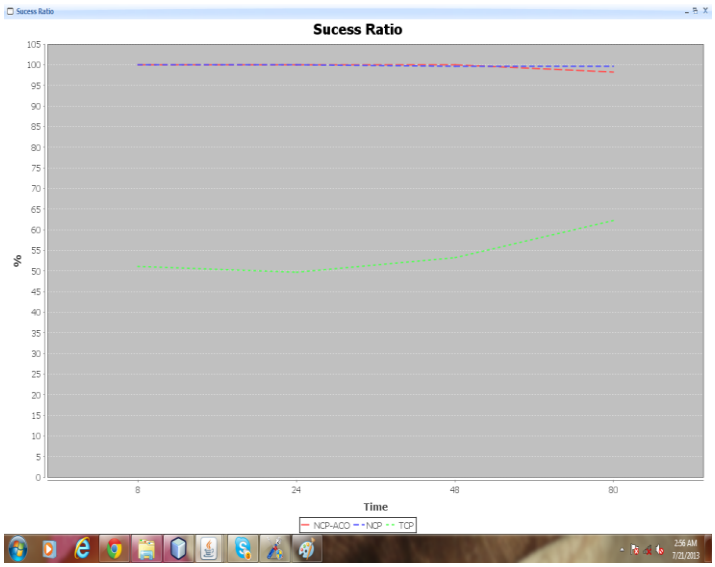

Figure 6: Success Ratio Wireless Network

REFERENCES

1. R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, Network information flow,[IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204121, Jul. 2000.
2. R. Koetter and M. Medard, BAn algebraic approach to network coding,[IEEE/ACM Trans. Netw., vol. 11, no. 5, pp. 782795, Oct. 2003.
3. S.-Y. Li, R. Yeung, and N. Cai, BLinear network coding,[IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371381,
4. T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, BA random linear network coding approach to multicast,[IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 44134430, Oct. 2006.
5. Y. Xi and E. M. Yeh, BDistributed algorithms for mini- mum cost multicast with networkcoding, in Proc. Allerton Annu. Conf. Commun. Control Comput, pp. 20732082, 2005.
6. D. Lun, N. Ratnakar, R. Koetter, M. Medard, E. Ahmed, and H. Lee, B Achieving minimum-cost multicast: A de- centralized approach based on network coding,[in Proc. IEEE Int. Conf. Comput. Commun., Mar. 2005, vol. 3 [8] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, Capacity of wireless erasure networks,[IEEE Trans. Inf. Theory, vol. 52, no. 3, Mar. 2006.
7. W. R. Stevens, TCP/IP Illustrated, Volume 1: The Proto- cols. Reading MA: Addison-Wesley, 1994.
8. D. S. Lun, B Efficient operation of coded packet networks,[Ph.D. dissertation, Dept. Electr. Eng. Comput. Sci., Mas- sachusetts Inst. Technol., Cambridge, MA, Jun. 2006.
9. G. R. Wright and W. R. Stevens, TCP/IP Illustrated, Volume 2: The Implementation. Reading, MA: Addison-Wesley,
10. S. Bhadra and S. Shakkottai, B Looking at large networks: Coding vs. Queuing, in Proc. IEEE Int. Conf. Comput. Commun, Apr. 2006, DOI: 10.1109/INFOCOM. 2006.
11. D. S. Lun and T. Ho, Network Coding: An Introduction. Cambridge, U.K.: Cambridge Univ. Press, 2008.

12. T. Ho, B Networking from a network coding perspective Ph.D. dissertation, Massachusetts Inst. Technol., Cambridge, MA, May 2004.
13. P. A. Chou, Y. Wu, and K. Jain, Practical network coding, in Proc. Allerton Conf. Commun. Control Comput., pp. Network coding: A historical perspective Yeung Proceedings of the IEEE Vol. 99,No. 3, March 2011
14. Linear network coding: Theory and algorithms By Shuo Yen Robert Li, Fellow IEEE, Qifu Tyler Sun, Member IEEE, and Ziyu Shao, Member IEEE Proceedings of the IEEE Vol. 99,No. 3, March 2011
15. Network coding and matroid theory Dougherty Proceedings of the IEEE Vol. 99,No. 3, March 2011
16. Theory and applications of network error correction coding Zhangs tutorial Proceedings of the IEEE Vol. 99, No.3, March 2011
17. Theory of secure network coding Cai and Chans Proceedings of the IEEE Vol. 99,No. 3, March 2011
18. Network coding meets TCP: Theory and implementation By Jay Kumar Sundararajan, Devavrat Shah, Muriel Medard, Fellow IEEE, Szymon Jakubczak, Michael Mitzenmacher, and Joao Barros Proceedings of the IEEE Vol. 99,No. 3, March 2011
19. Random network coding in peer-to peer networks: From theory to practice Finally, Li and Nius2011 Finally, Li and Nius Proceedings of the IEEE Vol. 99,No. 3, March 2011